DEPARTMENT OF THE ARMY
WASHINGTON, D.C. 20310

HQDA Ltr 25-99-1

SAIS-IAE

15 October 1999

Expires 15 October 2001

SUBJECT: U.S. Army Electronic Commerce Policy

SEE DISTRIBUTION

1. Purpose.

a. This letter provides Army policy regarding the development and implementation of Electronic Commerce (EC). It is effective immediately and applies to the active Army, the Army National Guard, and the U.S. Army Reserve for all administrative work-related processes that employ (or that will employ) EC techniques or technologies. This policy guidance will be formally incorporated into a future release of Army Regulation (AR) 25-1.

b. This letter also establishes the process by which the Army will manage and oversee proposed EC initiatives, within the constraints delineated in Paragraph 4 of this letter.

2. Proponent and exception authority. The proponent of this letter is the Director of Information Systems for Command, Control, Communications, and Computers (DISC4) (SAIS-ZA). The proponent has delegated exception authority to the Director of Electronic Commerce (SAIS-IAE) for all matters pertaining to Army EC and to the Director of CIO Integration (SAIS-IMC) for all matters pertaining to Army process improvement with a Command, Control, Communications, Computers, and Intelligence/Information Technology (C4I/IT) impact.

3. References.

a. Required publications.

(1) Army Regulation 70-1: Army Acquisition Policy, 15 Dec 97.

(2) Army Regulation 380-19: Information Systems Security, 27 Feb 98.

(3) The Army Electronic Commerce Strategic Plan, 10 Mar 98.

(4) Army Regulation 25-1: The Army Information Resources Management Program, 25 Mar 97.

(5) Joint Technical Architecture-Army, Version 5.5, 23 Dec 98.

(6) The Freedom of Information Act (5 USC 552 et seq.).

(7) Public Law 104-231: The Electronic Freedom of Information Act Amendments of 1996.

(8) Federal Acquisition Regulation (part 24).

(9) Army Regulation 340-21: The Army Privacy Program, 5 Jul 85.

(10) DOD Directive 5500.7-R: Joint Ethics Regulation, 30 Aug 93.

(11) DOD Directive 5230.9: Clearance of DOD Information for Public Release, 9 Apr 96.

(12) Army Regulation 25-400-2: The Modern Army Recordkeeping System, 26 Feb 93.

(13) Army Regulation 10-5: Organization and Functions (Headquarters, Department of the Army), 30 Nov 92.

b. Related publications.

(1) Army Regulation 310-25: Dictionary of United States Army Terms, 15 Oct 83.

(2) Section 850 of Public Law 105-85: National Defense Authorization Act for Fiscal Year 1998.

(3) General Order 10: Assignment of Functions, Responsibilities, and Duties Within the Army Secretariat, 12 Aug 97.

(4) OMB Circular A-130: Management of Federal Information Resources, 8 Feb 96.

(5) DOD Directive 8000.1: Defense Information Management Program, 27 Oct 92.

(6) Federal Acquisition Regulation (subpart 4.502).

(7) Memorandum on Central Contractor Registration (Director of Defense Procurement, 31 Mar 98).

(8) Public Law 104-134: Debt Collection Improvement Act of 1996.

(9) Public Law 104-106: Clinger-Cohen Act of 1996 (Public Law 104-208 redesignated Divisions D and E (the Information Technology Management Reform Act of 1996 and the Federal Acquisition Reform Act of 1996, respectively) of the DOD Authorization Act for FY96 (PL 104-106) as the Clinger-Cohen Act).

(10) Public Law 100-235: The Computer Security Act of 1987.

(11) OMB Bulletin 94-09: Payments by Electronic Funds Transfer, 15 Aug 94.

(12) FIPS Publication 161-2: Electronic Data Interchange, 22 May 96.

(13) Memorandum on the Use of the Ada Programming Language (ASD(C3I)), 29 Apr 97.

(14) Memorandum on Acquisition of Year 2000 (Y2K) Compliant Information Technology (IT) and Bringing Existing IT into Compliance (ASD(C3I)), 18 Dec 97.

(15) DOD Information Technology Management Strategic Plan, 20 Mar 97.

(16) DOD Regulation 5400.7-R: DOD Freedom of Information Act Program, 4 Sep 98.

(17) Army Regulation 15-1: Committee Management, 27 Nov 92.

(18) Army Regulation 71-9: Materiel Requirements, 30 Apr 97.

(19) Army Regulation 25-55: The Department of the Army Freedom of Information Act Program, 1 Nov 97.

(20) Army Regulation 602-2: Manpower and Personnel Integration (MANPRINT) in the System Acquisition Process, 7 Oct 94.

(21) FIPS Publication 140-1: Security Requirements for Cryptographic Modules, 11 Jan 94.

(22) FIPS Publication 186-1: Digital Signature Standard (DSS), 15 Dec 98.

(23) FIPS Publication 180-1: Secure Hash Standard (SHS), 17 Apr 95.

4. Responsibilities.

a. General.

(1) Headquarters, Department of the Army, and major Army commands (MACOMs)

shall use EC technologies to the maximum extent practicable to promote the goal of a paper-free (or near paper-free) business environment within the Army. (See also paragraphs b (Specific), c (Management Oversight), and d (Additional responsibilities) for additional responsibilities.)

(2) Proponents and materiel developers of Army EC initiatives shall prepare and submit to the Army EC Repository (maintained by SAIS-IAE) information describing these initiatives in a manner and format established by DISC4 (SAIS-IAE).

(3) In addition to the responsibilities assigned to materiel developers in the Army Electronic Commerce Strategic Plan (Reference 3a(3)), proponents of Army EC initiatives shall undertake the appropriate programming activities to ensure that their EC requirements can be adequately met.

(4) Proponents and materiel developers of Army EC initiatives shall comply fully with the provisions of this letter to ensure standardized implementation of EC throughout the Army unless specifically and formally granted an exception as explained in Paragraph 2.

b. Specific.

(1) *Process improvement.*

(a) Prior to procuring or implementing any Army EC solution, the proponent of the associated EC initiative shall conduct a process analysis and simplify the associated processes by eliminating those that add no value and, where possible, streamlining and integrating the others (Reference 3a(4)). Prior to initiating this process analysis, the proponent must satisfactorily address the following questions:

1. Does the process support core/priority mission functions?

2. Can the process be eliminated?

3. Can the process be accomplished more efficiently by another federal organization?

4. If the process is still needed, can its execution be outsourced in part?

5. If the process is still needed, can it be outsourced entirely?

(b) The process analysis must incorporate a life-cycle cost-benefit analysis (or an update thereto, as appropriate) (Reference 3b(4)). This cost-benefit analysis must include total costs for the initiative (including costs for the process analysis, the needed investments in information technology, and the full range of implementation costs, including those for operations and maintenance) and the expected investment benefits that would result from implementing the initiative (Reference 3b(5)).

(c) The proponent of an EC initiative shall perform a post-implementation review of the initiative and its resulting solution within two years of the final implementation to validate the estimated benefits and document effective management practices for broader use (Reference 3b(4)).

(2) *Authentication.*

(a) Army EC solutions shall be capable of ensuring authentication and confidentiality commensurate with the risk and magnitude of the harm from loss or unauthorized access to the information (Reference 3b(6)). Authentication control mechanisms selected for use (e.g., digital signature, password protection, public key cryptography, digital certificates) shall comply with the standards defined in the current version of the Joint Technical Architecture-Army (JTA-A) (Reference 3a(5)).

(b) For purposes of electronic funds transfer for payment of contractor invoices,

authentication of contractor identity and financial information shall be maintained in the Department of Defense (DOD) Central Contractor Registration database (Reference 3b(7)).

(3) *Intellectual property.* Proponents of Army EC initiatives, when designing and implementing an EC solution, must comply with the Federal requirements precluding the disclosure of proprietary information to unauthorized users (Reference 3b(4)). Army EC initiatives incorporating commercial-off-the-shelf (COTS) products within the EC solution shall comply with all data restrictions and copyright provisions accompanying said products.

(4) *Privacy.*

(a) Proponents designing and implementing EC solutions that contain information pertaining to individuals shall ensure that such information is not disclosed to or modified by unauthorized persons. Proponents shall (1) incorporate appropriate safeguards to limit the collection of information that identifies individuals to that which is legally authorized and necessary for the proper performance of the supported business functions and (2) limit the sharing of information that identifies individuals to that which is legally authorized (Reference 3b(4)).

(b) Any disclosure of information pertaining to individuals shall be done in accordance with the Freedom of Information Act (Reference 3a(6)), as amended by the Electronic FOIA Amendment of 1996 (Reference 3a(7)), Part 24 of the Federal Acquisition Regulation (FAR) (Reference 3a(8)), and the Army Privacy Program (Reference 3a(9)).

(c) Proponents designing and implementing EC solutions that collect or maintain information pertaining to individuals shall ensure that such information is accurate and correct (Reference 3a(4)).

(d) Dissemination of information pertaining to non-tax debts with the Federal Government shall comply with guidance issued by the Secretary of the Treasury (Reference 3b(8)).

(5) *Security.*

(a) Army EC solutions shall comply, at a minimum, with the provisions of the Secretary of Commerce's security standards (Reference 3b(9)), the Army Automated Information System Security Program (AISSP) (Reference 3a(2)), and the security provisions of the JTA-A (Reference 3a(5)). Proponents and materiel developers should consider such services as authentication, access control, data integrity, data confidentiality, non-repudiation, and availability (References 3a(4), 3a(5), and 3b(9)).

(b) Army EC solutions shall incorporate security features designed to control loss or unauthorized modification or disclosure of sensitive information commensurate with the risk and magnitude of the harm from loss, or unauthorized access to the information (References 3a(2), 3b(6), and 3b(10)).

(6) *Technology standards.*

(a) Army EC solutions shall comply with the standards specified in the JTA-A for the transfer of data and information to ensure that such solutions are based on commercial "open systems" architectures. Proponents and materiel developers of EC initiatives deviating from the JTA-A must receive a waiver from the Army CIO, or designee, prior to implementing such an initiative (Reference 3a(5)). In those instances in which the JTA-A does not state a standard, proponents and materiel developers shall comply with appropriate voluntary standards (Reference 3b(4)).

(b) EC solutions employing Electronic Funds Transfer (EFT) and Electronic Data Interchange (EDI) components shall comply with Federal Information Processing (FIPS) Publication 161-2 (Electronic Data Interchange), which requires the use of either the American National Standards Institute (ANSI) Accredited Standard Committee (ASC) X12 or

United Nations/Electronic Data Interchange for Administration, Commerce, and Transport (UN/EDIFACT) X12 data interchange standard (References 3b(11) and 3b(12)).

(c) Army EC solutions shall be based on the most appropriate programming language; however, the chosen language shall be selected in the context of system and software engineering factors that influence overall life-cycle costs, risks, and the potential for interoperability. In addition, such selections and the associated documentation of the decision process shall be subject to review during the milestone/system approval process (Reference 3b(13)).

(d) Proponents and materiel developers of Army EC initiatives that require compliance with a standard that does not reflect commercially accepted or Federally approved use (e.g., foreign national, state, local, or tribal government standards) shall request and receive an exception from the Army CIO, or designee, prior to implementing a solution conforming to such a standard.

(e) Proponents and materiel developers of Army EC initiatives shall undertake them in a manner that ensures Year 2000 (Y2K) compliance (References 3a(5) and 3b(14)).

(7) *Content.*

(a) Army EC solutions are intended for use in transacting official business. The use of Army EC solutions for official and approved non-official business shall be in accordance with the DOD Joint Ethics Program (Reference 3a(10)).

(b) Electronic dissemination of information for public release shall comply with DOD Directive (DODD) 5230.9, "Clearance of DOD Information for Public Release" (Reference 3a(11)). In those instances in which electronic information has been deleted for legitimate exemptions under The Freedom of Information Act or The Privacy Act prior to public release, the amount of such information shall be appropriately indicated (Reference 3a(7)).

(8) *Training.* Proponents and materiel developers of EC initiatives shall develop and maintain documentation on the resulting EC solution that describes both technical and functional features such that appropriate training for users and system administrators can be derived therefrom. Such training should address, at a minimum, system functions, maintaining information security, system maintenance, and protection against information warfare.

(9) *Transaction integrity and tracking.* Proponents and materiel developers of EC initiatives shall ensure that appropriate features are incorporated to ensure the preservation of data integrity throughout all electronic transactions (Reference 3b(4)). Such features should incorporate, at a minimum, transaction audit, message receipt, Recordkeeping, and non-repudiation functions.

(10) *Assured availability.*

(a) Proponents of EC initiatives shall develop and maintain contingency and crisis management plans for use in the event of system unavailability. Proponents shall conduct such planning efforts commensurate with the criticality of the information within the EC solution (Reference 3b(5)).

(b) Proponents of EC initiatives shall comply with the requirements of the Vital Records Program to ensure that information required by headquarters is available for essential operation during a national emergency (Reference 3a(4)).

(11) *Recordkeeping.* Proponents of EC initiatives shall ensure that they design, develop, and implement EC solutions to incorporate economical and efficient record management and archival functions. Proponents shall manage EC records in accordance

with the Army Information Resources Management Program (Reference 3a(4)) and the Modern Army Recordkeeping System (MARKS) (Reference 3a(12)). As part of the archiving program, proponents shall archive a copy of the associated executable program(s) to ensure future access to data manipulated by EC solutions (Reference 3a(4)).

(12) *Support infrastructure.* Proponents and materiel developers of Army EC initiatives shall ensure that the support infrastructure is adequate to accommodate the resulting solution without significant degradation of other services provided through the infrastructure (Reference 3b(15)). If necessary, proponents and materiel developers shall plan for and fund the needed infrastructure enhancements to ensure that degradation of services does not occur upon implementation of the proposed EC solution. Moreover, such enhancements shall incorporate the total package of needed resources (e.g., new equipment training, databases, documentation, logistics support), not merely the prime mission automation IT. Such enhancements shall also adequately accommodate the new system's compatibility, interoperability, and integration with the existing support infrastructure, including the installation's information infrastructure. Any such enhancements or modifications to the support infrastructure shall comply with the specifications defined in the current version of the JTA-A (Reference 3a(5)).

c. Management oversight.

(1) *HQDA oversight.* Several entities within the Enterprise Strategy Control Structure (ESCS) will perform reviews of existing and planned EC initiatives for the purposes of identifying and prioritizing potential opportunities to improve cross-functional integration within the Army. Participants in this process include: (1) the Army Command, Control, Communications, Computers, and Intelligence (C4I) Executive Board, comprising three-star representatives from the Secretariat, ARSTAF, and the MACOMs; (2) the Enterprise General Officer Steering Committee (GOSC), comprising one- and two-star representatives from the Secretariat, ARSTAF, and MACOMs; and (3) the Electronic Commerce Integrated Process Team (EC IPT), comprising GS-15/O-6 representatives from the Secretariat, ARSTAF, and the MACOMs. Using the information contained in the EC repository (see paragraph 5a(2) for requirements for providing such information), the EC IPT shall review existing and planned EC initiatives, identify and prioritize potential opportunities to improve cross-functional integration, and provide its recommendations for improving cross-functional integration to the GOSC. The GOSC shall review and approve or disapprove EC IPT recommendations, revising them as appropriate. As required, the GOSC may also forward its recommendations to the Army C4I Executive Board for further consideration and review if the GOSC determines that such elevation would serve the Army's best interests with respect to its strategic EC direction.

(2) *MACOM oversight.* Major Army commands shall establish analogous oversight procedures for EC initiatives under their purview to increase MACOM-specific cross-functional integration. MACOMs shall provide information describing EC initiatives under their purview to the EC IPT in a manner and time to be established by the DISC4 (SAIS-IAE). Such information shall include, at a minimum, a description of the initiative and the process(es) it supports, expected life-cycle cost and benefits, and expected applicability (i.e., specific to the MACOM or applicable to two or more MACOMs).

d. Additional responsibilities. In addition to, and not superseding, the roles and responsibilities assigned in AR 10-5 (Reference 3a(13)), AR 25-1 (Reference 3a(4)), AR 70-1 (Reference 3a(1)), and elsewhere in this document, Army organizations enumerated in the remainder of this paragraph shall assume the following additional roles and responsibilities with respect to EC.

(1) The Director of Information Systems for Command, Control, Communications, and Computers shall:

(a) Serve as the single focal point for all EC activities within the Department of the

Army and manage and execute the Army Electronic Commerce Program (including review and general oversight of EC planning, performance measurement, activities, initiatives, and solutions) (SAIS-IAE).

(b) Serve as the liaison between (1) the Office of the Secretary of Defense (OSD) and the Military Departments and (2) the OSA, the ARSTAF, the MACOMs, and the Army supported Commanders-in-Chief (CINCs) (United States European Command (USEUCOM) and United States Southern Command (USSOUTHCOM)) and all other CINCs to ensure the Army meets its obligations as a Joint Force provider for all issues pertaining to Army EC programs, policies, and standards (SAIS-IAE).

(c) Coordinate with and provide advice and guidance, as needed, to the DOD CIO (ASD(C3I)) in the development and maintenance of DOD EC plans and policies (SAIS-IAE).

(d) Coordinate with OSD concerning the development, implementation, and maintenance of common EC capabilities in the Defense Information Infrastructure to ensure that Army-wide interests are being served (SAIS-IAE).

(e) Develop EC planning guidance for inclusion within the Army's Planning, Programming, Budgeting, and Execution System; the Army Long Range Planning Guidance; the Army Modernization Plan; the Requirements Determination Process; the Army Research, Development, and Acquisition Plan; The Army Plan; and the Army Program Guidance Memorandum (SAIS-IAE).

(f) Participate, as required, in international, national, other Federal, and DOD EC development activities, programs, policies, initiatives, and standards bodies (SAIS-IAE).

(g) Coordinate functional participation in Federal, DOD, Department of the Army, and related EC working groups, standards bodies, and consortiums (SAIS-IAE).

(h) Participate, as needed, in other Federal government agency and industry forums concerning EC architecture, infrastructures, and shared data systems to ensure that the Government-wide EC program remains in concert with private industry (SAIS-IAE).

(i) Exercise oversight responsibility to ensure that all EC-related C4I/IT initiatives comply with the JTA-A (SAIS-PAA).

(j) Ensure that the JTA-A reflects industry EC standards and COTS solutions to the maximum extent practicable (SAIS-PAA).

(k) Coordinate with OSD to update the DOD Joint Technical Architecture to ensure that Army JTA-A views are reflected to the maximum extent possible (SAIS-PAA).

(l) Develop and promulgate requirements for providing information on EC initiatives to the Army EC Repository (SAIS-IAE).

(m) Develop guidance and provide assistance to proponents of EC initiatives regarding the use of voluntary standards (SAIS-PAA).

(n) Conduct an annual assessment of existing COTS solutions to promote the use of commercial EC products that reduce costs and enhance efficiencies (SAIS-IAE).

(o) Sponsor a biennial study to identify, evaluate, and address security and infrastructure concerns with respect to EC initiatives (SAIS-IAS).

(p) Develop guidance and provide assistance to proponents of EC initiatives regarding the integration and use of transaction audit methods to ensure the transaction integrity of a particular EC solution (SAIS-IAS).

(q) Develop guidance and provide assistance to proponents of EC initiatives to

evaluate a particular initiative's potential effect on the ability of the existing information technology infrastructure to continue to operate without significant degradation in quality of service (SAIS-PAA).

(r) Coordinate with the Civilian Career Program Functional Chiefs/Functional Chief Representatives to identify and analyze EC training requirements for the Total Army Workforce at the technical, managerial, and executive levels (SAIS-IAE).

(s) Provide the results of process improvement efforts to OSD (ASD(C3I)) for incorporation in the OSD EC operational architecture (SAIS-IAE).

(t) Maintain and make available information describing the computer and communications infrastructure and related services that are currently available from the Defense Information Systems Agency/Defense Logistics Agency (DISA/DLA) to support EC requirements (SAIS-IAE).

(u) Maintain and make available to the OSA, the ARSTAF, and the MACOMs a repository of current and planned EC initiatives and lessons learned (SAIS-IAE).

(v) Serve as the Chair of the EC IPT (SAIS-IAE).

(2) Each office within the Army Secretariat shall:

(a) Serve as the functional proponent for EC initiatives within its assigned areas of functional responsibility.

(b) Undertake appropriate process improvement activities within its assigned area of functional responsibility for each EC initiative; review and implement best business practices in support of EC initiatives; and provide the results of process improvement efforts to DISC4 (SAIS-IAE) for incorporation within the OSD EC operational architecture.

(c) Coordinate its needs for DISA/DLA-provided computer and communications infrastructure and related services to support its EC requirements with DISC4 (SAIS-IAE).

(d) Designate appropriate personnel to serve as members of the EC IPT.

(e) When undertaking EC initiatives, in coordination with DISC4 (SAIS-IAE), develop training and educational requirements for both soldiers and Army civilians on EC within its assigned area of responsibility.

(f) Implement EC initiatives that comply with existing legal mandates and directives, including the specific policy provisions of this letter as established in paragraphs 5a and 5b.

(g) When undertaking EC initiatives, prescribe requirements for using EC technologies to the maximum extent practicable in all facets of system design, development, and operations within its assigned functional areas of responsibility.

(h) When undertaking EC initiatives, plan, program, and budget for EC initiatives and implementation within its respective functional communities in compliance with the Army POM Preparation Instructions.

(3) Each office within the Army Staff shall:

(a) Serve as the Headquarters, Department of the Army (HQDA) subject area functional proponent for all EC initiatives systems requirements, development, and operations within their respective assigned areas of functional responsibility.

(b) Provide the necessary guidance and oversight on process improvement initiatives within their respective areas of functional responsibility; provide the results of process improvement efforts to DISC4 (SAIS-IAE) for incorporation within the OSD EC operational architecture.

(c) Coordinate its needs for DISA/DLA-provided computer and communications infrastructure and related services to support its EC requirements with DISC4 (SAIS-IAE).

(d) Prescribe requirements for using EC technologies to the maximum extent

practicable in all facets of system design, development, and operations within their respective areas of functional responsibility.

(e) Implement EC initiatives that comply with existing legal mandates and directives, including the specific policy provisions of this letter as established in paragraphs 5a and 5b.

(f) Designate appropriate personnel to serve as members of the EC IPT.

(g) In coordination with DISC4 (SAIS-IAE), develop training and educational requirements for both soldiers and Army civilians on EC within its assigned area of responsibility.

(h) Plan, program, and budget for EC initiatives and implementation within their respective functional communities in compliance with the Army Program Objective Memorandum (POM) Preparation Instructions.

(i) In addition to the above listed responsibilities, the Deputy Chief of Staff for Personnel (DCSPER) shall:

1. Develop, publish, and maintain appropriate records management policies and programs for records generated and stored within EC solutions.

2. Develop, publish, and maintain appropriate privacy policies and programs for records generated and stored within EC solutions.

(4) Materiel developers shall:

(a) Implement EC technologies in accordance with functional requirements to the maximum extent practicable in all facets of developing, fielding, training, integrating, and testing new and upgraded technical solutions that interface with Army trading partners (including DOD, other Federal agencies, and industry, as appropriate) or with other Army functional areas.

(b) Ensure that actions involving implementation of EC initiatives comply with existing legal mandates and directives, including the specific policy provisions of this letter as established in paragraphs 5a and 5b.

(c) Coordinate with DISC4 (SAIS-IAE) and the Civilian Career Program Functional Chiefs and Functional Chief Representatives in identifying EC training requirements for new fielded equipment.

(d) Provide DISC4 (SAIS-IAE) input for the EC repository to maintain a central knowledge base of current EC initiatives, techniques, and concepts that can be promulgated throughout the Army.

(e) Recommend to the DISC4 (SAIS-PAA) appropriate EC standards for inclusion within the JTA-A.

(5) The major Army commands shall:

(a) Undertake MACOM-unique process improvement initiatives within their respective communities; in accomplishing such initiatives, review and implement best practices; and provide the results of process improvement efforts to DISC4 (SAIS-IAE) for incorporation within the OSD EC operational architecture.

(b) Coordinate its needs for DISA/DLA-provided computer and communications infrastructure and related services to support its EC requirements with DISC4 (SAIS-IAE).

(c) Implement EC technologies to the maximum extent practicable in all facets of system design, development, and operations for MACOM-unique requirements.

(d) Ensure that actions involving implementation of EC initiatives comply with existing legal mandates and directives, including the specific policy provisions of this letter as established in paragraphs 5a and 5b.

(e) Designate appropriate personnel to serve as members of the EC IPT.

(f) Plan, program, and budget for EC initiatives and implementation within their respective organizations in compliance with the MACOM POM Development Instructions and Program Budget Guidance (PBG), and incorporate specific requirements into their respective MACOM POM submissions.

(g) Provide DISC4 (SAIS-IAE) input for the EC repository to maintain a central knowledge base of current EC initiatives, techniques, and concepts that can be promulgated throughout the Army.

(h) In addition to the above listed responsibilities, TRADOC shall, in coordination with the DISC4 (SAIS-IAE) and Materiel Developers, identify and analyze EC training requirements and, when appropriate, update existing courseware.

(6) The Electronic Commerce Integrated Process Team shall develop guidance and provide assistance to proponents of EC initiatives with regard to providing information on their respective initiative(s) to the EC IPT for review and forwarding to the GOSC and the Army C4I Executive Board.

Glossary

Section I
Abbreviations

AISSP
Automated Information System Security Program

ANSI
American National Standards Institute

AR
Army Regulation

ARSTAF
The Army Staff

ASC
Accredited Standard Committee

ASD
Assistant Secretary of Defense

C3I
Command, Control, Communications, and Intelligence

C4I
Command, Control, Communications, Computers, and Intelligence

CFR
Code of Federal Regulations

CINC
Commander in Chief

CIO
Chief Information Officer

COTS
Commercial-Off-the-Shelf

DCSPER
Deputy Chief of Staff for Personnel

DISA
Defense Information Systems Agency

DISC4
Director of Information Systems for Command, Control, Communications, and Computers

DLA
Defense Logistics Agency

DOD
Department of Defense

DODD
Department of Defense Directive

EC
Electronic Commerce

EC IPT
Electronic Commerce Integrated Process Team

EDI
Electronic Data Interchange

EDIFACT
Electronic Data Interchange for Administration, Commerce, and Transport

EFT
Electronic Funds Transfer

ESCS
Enterprise Strategy Control Structure

FAR
Federal Acquisition Regulation

FIPS
Federal Information Processing Standards

FOIA
Freedom of Information Act

GOSC
General Officer Steering Committee

HQDA
Headquarters, Department of the Army

IT
Information Technology

ITMRA
Information Technology Management Reform Act

JTA-A
Joint Technical Architecture-Army

MACOM
Major Army Command

MARKS
Modern Army Recordkeeping System

OMB
Office of Management and Budget

OSA
Office of the Secretary of the Army

PBG
Program Budget Guidance

POM
Program Objective Memorandum

TRADOC
Training and Doctrine Command

UN
United Nations

USEUCOM
United States European Command

USSOUTHCOM
United States Southern Command

Section II
Terms
Processes associated with raising, organizing, training, equipping, deploying, and sustaining the Army in the accomplishment of its mission.

Army Staff
That portion of the staff of the Secretary of the Army at the seat of government, which is presided over by the Chief of Staff (Reference 3b(1)).

Business transaction
An exchange or transfer of information or data that supports an administrative work-related process.

Electronic commerce
Army EC is "electronic techniques for accomplishing business transactions, including electronic mail or messaging, World Wide Web technology, electronic bulletin boards,

purchase cards, electronic funds transfers, and electronic data interchange" (Reference 3b(2)).Electronic commerce initiative-an Army EC Initiative is the use of electronic techniques to accomplish Army business transactions in support of defined mission objectives.

Electronic commerce solution
An EC solution is the resulting product of an EC initiative.

Electronic data interchange
A subset of EC involving the computer-to-computer communication of data that permits the receiver to perform the function of a standard business transaction and is in a predefined standard data format.

Functional proponent
The Army Staff agency responsible for the subject area in which automation is used or is to be used, including automation in support of the function performed (Reference 3b(1)).

Materiel developer
The Research, Development, and Acquisition command, agency, or office assigned responsibility for the system under development or being acquired (Reference 3a(1)).

Office of the Secretary of the Army
The Under Secretary of the Army; the Deputy Under Secretaries of the Army; the Assistant Secretaries of the Army; the Administrative Assistant to the Secretary of the Army; the General Counsel of the Army; the Director of Information Systems for Command, Control, Communications, and Computers; the Inspector General; the Auditor General; the Chief of Legislative Liaison; the Chief of Public Affairs; and the Director, Office of Small and Disadvantaged Business Utilization (Reference 3b(3)).

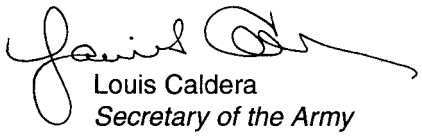
Process improvement
Any systematic, disciplined improvement approach that critically examines, rethinks, and redesigns mission-delivery processes to achieve performance improvements in areas important to customers and other stakeholders.

Proponent
An Army organization or staff that has been assigned primary responsibility for material or subject matter in its area of interest (e.g., proponent school, proponent staff agency, proponent center); an Army organization or staff that has been charged with accomplishment of a task (Reference 3b(1)).

Sensitive Information
Unclassified information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act (Reference 3a(2)).

Standard
A technical specification or other document drawn up with the cooperation and consensus or general approval of all parties affected by it, based upon the consolidated results of

science, technology, and experience, aimed at the promotion of optimum community benefits and approved by a standardization body.



Louis Caldera
Secretary of the Army

Distribution:

HQDA (SACW)
HQDA (SAFM)
HQDA (SAIE)
HQDA (SAMR)
HQDA (SAAL)
HQDA (SAGC)
HQDA (SAAA)
HQDA (SAIS-ZA)
HQDA (SAIG-ZA)
HQDA (SAAG-ZA)
HQDA (SAUS-IA)
HQDA (SAUS-OR)
HQDA (SALL)
HQDA (SAPA)
HQDA (SADBU)
HQDA (DAMI-ZA)
HQDA (DALO-ZA)
HQDA (DAMO-ZA)
HQDA (DAPE-ZA)
HQDA (DAEN-ZA)
HQDA (DASG-ZA)
HQDA (NGB-ZA)
HQDA (DAAR-ZA)
HQDA (DAJA-ZA)
HQDA (DACH-ZA)
HQDA (DAIM-ZA)

COMMANDER IN CHIEF
U.S. ARMY EUROPE AND SEVENTH ARMY

COMMANDERS
EIGHTH U.S. ARMY
FORCES COMMAND
U.S. ARMY MATERIEL COMMAND
U.S. ARMY TRAINING AND DOCTRINE COMMAND

U.S. ARMY CORPS OF ENGINEERS
U.S. ARMY SPECIAL OPERATIONS COMMAND
U.S. ARMY PACIFIC
MILITARY TRAFFIC MANAGEMENT COMMAND
U.S. ARMY CRIMINAL INVESTIGATION COMMAND
U.S. ARMY MEDICAL COMMAND
U.S. ARMY INTELLIGENCE AND SECURITY COMMAND
U.S. ARMY MILITARY DISTRICT OF WASHINGTON
U.S. ARMY SOUTH

CF:

COMMANDER IN CHIEF
U.S. SOUTHERN COMMAND
U.S. EUROPEAN COMMAND

PROGRAM EXECUTIVE OFFICE
COMMAND, CONTROL & COMMUNICATIONS SYSTEMS

USAPA

ELECTRONIC PUBLISHING SYSTEM
TEXT FORMATTER ... Version 2.61

PIN:
DATE: 10-20-99
TIME: 17:02:51
PAGES SET: 17

DATA FILE: 25991.fil
DOCUMENT:
DOC STATUS: NEW PUBLICATION